```
File 348:EUROPEAN PATENTS 1978-2004/Dec W02
         (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20041216,UT=20041209
         (c) 2004 WIPO/Univentio

Set     Items   Description
S1     284776   CODE OR CODES OR CODED OR CODING? ? OR SUBCOD???? ?
S2    1231146   NUMBER? ? OR NUMERAL? ? OR NUMERIC?? ? OR ALPHANUMERIC? OR
            INTEGER? ? OR DIGIT? ? OR VALUE OR VALUES
S3     830126   SEQUENCE? OR SEQUENT? OR BIT OR BITS OR SUBSEQUEN? OR STRI-
            NG? ? OR STRINGS
S4     925795   POINT? OR IDENTIFIER? ? OR SUBKEY? ? OR SUB()KEY? ?
S5      30120   S1:S2(3N)ADDITIONAL
S6         56   MICROCOD???? ?(3N)ADDITIONAL
S7      30959   (S1:S2 OR MICROD???? ?)(3N)(AUXILAR? OR AUXILIAR? OR AUXIL-
            L? OR ADJUNCT? OR ANCILLAR? OR ANCILLIA? OR SUPPLEMENT? OR IN-
            DEX??? ?)
S8     262560   KEY? ? OR CIPHER? ? OR CYPHER? ? OR ALGORITHM? OR KEYPAIR?
S9      25116   S8(3N)(PARTIAL? OR PORTION? ? OR FRAGMENT? OR SECTION? OR -
            PARTITION? OR PIECE? ? OR PART OR PARTS OR COMPONENT? OR SUBC-
            OMPONENT?)
S10      2726   S8(3N)(SUBSET? OR SUB()SET? ? OR SEGMENT? OR FRACTION?)
S11      2191   S9:S10(5N)(GENERAT? OR DERIV??? ? OR DERIVAT? OR PRODUCE? ?
            OR PRODUCING OR PRODUCTION? ? OR PROD? ? OR CREAT???? ? OR C-
            ONSTRUCT?)
S12      1925   S9:S10(5N)(FORM OR FORMS OR FORMED OR FORMING OR FORMATION?
            ? OR SYNTHESIS? OR SYNTHESIZ? OR ORIGINAT? OR DEVELOP?)
S13     54207   (S1:S3 OR MICROCOD???? ?)(3N)ADDITIONAL
S14     37702   (S1:S3 OR MICROD???? ?)(3N)(AUXILAR? OR AUXILIAR? OR AUXIL-
            L? OR ADJUNCT? OR ANCILLAR? OR ANCILLIA? OR SUPPLEMENT? OR IN-
            DEX??? ?)
S15       273   S11:S12(25N)(S4 OR S13:S14)
S16     21554   S8(5N)(ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR DECOD???? ? OR
            ENCOD???? ? OR INCOD???? ? OR UNENCOD? OR UNINCOD? OR DECRYP-
            T?)
S17      1299   S8(5N)(UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR DECIPHE-
            R? OR DECYPHER? OR UNCRYPT? OR UNCIPHER? OR UNCYPHER? OR UNCO-
            D???? ?)
S18        50   S15(25N)S16:S17
S19      6945   IC='H04L-009'
S20        26   S18 AND S19
S21        13   S18/TI,AB,CM
S22        32   S20:S21
S23        18   S18 NOT S22
S24        18   IDPAT (sorted in duplicate/non-duplicate order)
S25        17   IDPAT (primary/non-duplicate records only)
```

? t22/5,k/4-5

22/5,K/4 (Item 4 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01516132
Method and apparatus for symmetric encryption/decryption of recorded data
Verfahren und Vorrichtung zur symmetrischen Verschlusselung/Entschlusselung von aufgezeichneten Daten
Methode et dispositif de cryptage/decryptage symmetrique de donnees enregistrees
PATENT ASSIGNEE:
Sony Computer Entertainment Inc., (3064090), 7-1-1 Akasaka, Minato-ku, Tokyo 107-0052, (JP), (Applicant designated States: all)
Sony Corporation, (214031), 6-7-35 Kitashinagawa, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)
INVENTOR:
Asano, Tomoyuki, c/o Sony Corporation, 6-7-35 Kitashinagawa, Shinagawa-Ku, Tokyo 141-0001, (JP)
Ishibashi, Yoshihito, c/o Sony Corporation, 6-7-35 Kitashinagawa, Shinagawa-Ku, Tokyo 141-0001, (JP)
Shirai, Taizo, c/o Sony Corporation, 6-7-35 Kitashinagawa, Shinagawa-Ku, Tokyo 141-0001, (JP)
Akishita, Toru, c/o Sony Corporation, 6-7-35 Kitashinagawa, Shinagawa-Ku, Tokyo 141-0001, (JP)
Yoshimori, Masaharu, c/o Sony Computer Entertainment, 7-1-1 Akasaka, Minato-ku, Tokyo 107-0052, (JP)
Tanaka, Makoto, c/o Sony Computer Entertainment, 7-1-1 Akasaka, Minato-ku, Tokyo 107-0052, (JP)
LEGAL REPRESENTATIVE:
Robinson, Nigel Alexander Julian et al (69551), D. Young & Co., 21 New Fetter Lane, London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 1267515 A2 021218 (Basic)
EP 1267515 A3 040407
APPLICATION (CC, No, Date): EP 2002078475 010119;
PRIORITY (CC, No, Date): JP 200013322 000121; JP 200015551 000125; JP 200015858 000125; JP 200016029 000125; JP 200016213 000125; JP 200016251 000125; JP 200016292 000125
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
RELATED PARENT NUMBER(S) - PN (AN):
EP 1195734 (EP 2001901463)
INTERNATIONAL PATENT CLASS: **H04L-009/06** ; **H04L-009/32** ; G11B-020/00

ABSTRACT EP 1267515 A2
A record reproducing player and save data processing methods capable of insuring security of save data are provided. Save data is stored in a recording device, encrypted with the use of a program's individual encryption key, e.g., a content key, or a save data encryption key created based the content key, and when reproducing the save data a decryption process is conducted on it with the use of the save data decryption key particular to the program. Furthermore, it is made possible to create save data encryption keys based on a variety of restriction information, such as performing the storing and reproducing of the save data by conducting encryption and decryption on the save data with the save data encryption keys and decryption keys created with the use of a record reproducing player's individual key or a user's password.
ABSTRACT WORD COUNT: 140
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	021218 A2	Published application without search report
Assignee:	030108 A2	Transfer of rights to new applicant: Sony Computer Entertainment Inc. (3064090) 7-1-1 Akasaka, Minato-ku Tokyo 107-0052 JP Sony Corporation (214031) 6-7-35 Kitashinagawa, Shinagawa-ku Tokyo 141-0001 JP
Change:	030305 A2	Inventor information changed: 20030114
Change:	031217 A2	International Patent Classification changed: 20031031
Search Report:	040407 A3	Separate publication of the search report
Examination:	041117 A2	Date of request for examination: 20040921

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200251	6596
SPEC A	(English)	200251	73431
Total word count - document A			80027
Total word count - document B			0
Total word count - documents A + B			80027

INTERNATIONAL PATENT CLASS: **H04L-009/06** ...

... **H04L-009/32**

...SPECIFICATION data processing executed by the data processing apparatus is signature processing on data, the key **generating** step is a signature **key generating** step of executing **encryption** processing based on a signature **key generation** master key MKdev for **generating** a data processing apparatus signature **key** Kdev of the data processing apparatus and a data processing apparatus **identifier** , which is identification data of the data processing apparatus and generating the data processing apparatus...

...key based on a distribution key generation master key for generating a contents data distribution **key** used for **encryption** processing on contents data and a contents **identifier** , which is the **identifier** of the provided contents data and executes encryption processing on the contents data, and the contents data utilization apparatus **generates** a contents data distribution **key** based on the distribution key **generation** master key and a contents **identifier** , which is the **identifier** of the provided contents data and executes decryption processing on the contents data.

Furthermore, according...comprises a recording data processing apparatus signature key master key MKdev and data processing apparatus **identifier** IDdev, characterized in that the **encryption** processing section **generates** a signature **key** Kdev as the data processing apparatus specific **key** through **encryption** processing based on the recording data processing apparatus signature key master key MKdev and the data processing apparatus **identifier** IDdev.

Furthermore, in another embodiment of the data processing apparatus of the present invention, the **encryption** processing **section generates** the signature **key** Kdev through DES **encryption** processing applying the recording data processing apparatus signature key master key MKdev to the data processing apparatus **identifier** IDdev.

Furthermore, in another embodiment of the data processing apparatus of the present invention, the...

22/5,K/5 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01504244
DATA ACCESS MANAGEMENT SYSTEM AND MANAGEMENT METHOD USING ACCESS CONTROL TICKET
DATENZUGRIFFSMANAGEMENTSYSTEM UND MANAGEMENTVERFAHREN MIT EINEM ZUGRIFFSSTEUERTICKET
SYSTEME DE GESTION D'ACCES AUX DONNEES ET PROCEDE DE GESTION UTILISANT UN BILLET DE COMMANDE D'ACCES
PATENT ASSIGNEE:
Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)
INVENTOR:
YOSHINO, Kenji, c/o Sony Corporation, 7-35, Kitashinagawa 6-Chome, Shinagawa-Ku, Tokyo 141-0001, (JP)
Ishibashi, Yoshihito, c/o Sony Corporation, 7-35, K itashinagawa 6-Chome, Shinagawa-Ku, Tokyo 141-0001, (JP)
SHIRAI, Taizo, c/o SONY CORPORATION, 7-35, Kitashinagawa 6-Chome, Shinagawa-Ku, Tokyo 141-0001, (JP)
TAKADA, Masayuki, c/o Sony Corporation, 7-35, Kitashinagawa 6-Chome, Shinagawa-Ku, Tokyo 141-0001, (JP)
LEGAL REPRESENTATIVE:
Robinson, Nigel Alexander Julian et al (69551), D. Young & Co., 21 New Fetter Lane, London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 1303075 A1 030416 (Basic)
WO 2002076013 020926
APPLICATION (CC, No, Date): EP 2002702791 020307; WO 2002JP2113 020307
PRIORITY (CC, No, Date): JP 200173353 010315
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **H04L-009/00** ; G09C-001/00; G06F-012/14; G06F-015/00; G06F-017/60; G06F-019/00; G06F-017/00; G06K-019/00

ABSTRACT EP 1303075 A1
To provide a data access management system that enables access control management for data files stored in a memory of a device. The system manages data access processing performed by an access unit for a memory-loaded device, and issues a service permission ticket (SPT), which serves as an access control ticket in which an access mode to be accepted for the access unit, such as a reader/writer, is set. The memory-loaded device receives the service permission ticket (SPT) from the access unit, and performs processing according to the access mode indicated in the service permission ticket (SPT). The service permission tickets (SPTs) in which access modes to be accepted for the access units are set are individually issued according to the access units. Accordingly, various modes of access according to the access units can be executed.
ABSTRACT WORD COUNT: 137
NOTE:
Figure number on first page: 0001

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 021120 A1 International application. (Art. 158(1))
Application: 021120 A1 International application entering European phase
Application: 030416 A1 Published application with search report
Examination: 030416 A1 Date of request for examination: 20021031
LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200316	8394
SPEC A	(English)	200316	79434
Total word count - document A			87828
Total word count - document B			0
Total word count - documents A + B			87828

INTERNATIONAL PATENT CLASS: **H04L-009/00 ...**

...SPECIFICATION S659), the device creates a pair of a public key (PUB PAR) and a private **key** (PRI PAR) by using the **encryption** processor (see Fig. 5) in the, device, and writes the **created keys** into the **partition key** area (see Fig. 23) (S660). Then, the device makes adjustments of the **pointer** , the size, and the free block number in device, which are required due to the...
? t22/5,k/12,18

22/5,K/12 (Item 12 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00421296
Transaction system security method and apparatus.
Sicherheitsvorrichtung und -verfahren fur Transaktionssystem.
Methode et appareil de securite pour un systeme de transactions.
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: DE;FR;GB;IT)
INVENTOR:
Abraham, Dennis George, 5795 Gettysburg Drive, Concord, North Carolina, 28025, (US)
Aden, Steven George, 5641 Mallard Drive, Charlotte, North Carolina 28227, (US)
Arnold, Todd Weston, 2008 Bantry Lane, Charlotte, North Carolina 28213, (US)
Neckyfarow, Steven William, 16 Chevron Drive, Charlotte, North Carolina 28211, (US)
Rohland, William Stanley, 4234 Rotunda Road, Charlotte, North Carolina 28226, (US)
LEGAL REPRESENTATIVE:
Schafer, Wolfgang, Dipl.-Ing. (62021), IBM Deutschland Informationssysteme GmbH Patentwesen und Urheberrecht, D-70548 Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 421409 A2 910410 (Basic)
EP 421409 A3 910529
APPLICATION (CC, No, Date): EP 90119012 901004;
PRIORITY (CC, No, Date): US 418068 891006
DESIGNATED STATES: DE; FR; GB; IT
INTERNATIONAL PATENT CLASS: G07F-007/10; G06F-001/00; G06F-015/30; **H04L-009/32**
CITED PATENTS (EP A): GB 2204971 A; EP 165789 A
CITED REFERENCES (EP A):
COMPUTERS & SECURITY. vol. 6, no. 5, 1987, AMSTERDAM NL pages 385 - 395; spender: "identifying computer users with authentication devices (tokens)";

ABSTRACT EP 421409 A2
An improved security system is disclosed which uses especially an IC card to enhance the security functions involving component authentication, user verification, user authorization and access control,

protection of message secrecy and integrity, management of cryptographic keys, and auditablity. Both the security method and the apparatus for embodying these functions across a total system or network using a common cryptographic architecture are disclosed. Authorization to perform these functions in the various security component device nodes in the network can be distributed to the various nodes at which they will be executed in order to personalize the use of the components.
ABSTRACT WORD COUNT: 104

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	910410	A2	Published application (A1with Search Report ;A2without Search Report)
Examination:	910410	A2	Date of filing of request for examination: 901213
Search Report:	910529	A3	Separate publication of the European or International search report
Examination:	930929	A2	Date of despatch of first examination report: 930813
Change:	940921	A2	Representative (change)
Withdrawal:	971029	A2	Date on which the European patent application was deemed to be withdrawn: 970501

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	1082
SPEC A	(English)	EPABF1	8287
Total word count - document A			9369
Total word count - document B			0
Total word count - documents A + B			9369

...INTERNATIONAL PATENT CLASS: **H04L-009/32**

...SPECIFICATION keys in secure fashion in order to initialize the security processor. That, after the master **key** entered in **pàrts** , is used to **generate** other keys for distribution to other devices at other nodes in the secure network.
The directory server task 157 contains the **pointers** and program routines to allow the security server to access **encryption keys** and other information needed to perform its cryptographic functions, interfacing with PC DOS file access...

22/5,K/18 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01093477 **Image available**
METHOD AND APPARATUS FOR SECURE E-MAIL
PROCEDE ET DISPOSITIF PERMETTANT DE SECURISER LE COURRIER ELECTRONIQUE
Patent Applicant/Assignee:
KRYPTIQ CORPORATION, 1920 NW Amberglen Pkwy., Suite 100, Beaverton, OR 97006, US, US (Residence), US (Nationality)
Inventor(s):
KARAMCHEDU Murali M, 14825 SW Millikan Way, #1425, Beaverton, OR 97006, US,
SPONAUGLE Jeffrey B, 2617 NE Nova Avenue, Hillsboro, OR 97124, US,
Legal Representative:
KLINDTWORTH Jason K (et al) (agent), Schwabe, Williamson & Wyatt, P.C., Pacwest Center, Suites 1600-1900, 1211 SW Fifth Avenue, Portland, OR 97204, US,
Patent and Priority Information (Country, Number, Date):

Patent: WO 200415943 A1 20040219 (WO 0415943)
Application: WO 2003US24540 20030806 (PCT/WO US03024540)
Priority Application: US 2002401945 20020807; US 2003394446 20030320
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PG PH PL PT RO RU SC SD
SE SG SK SL SY TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE
SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/58
International Patent Class: H04L-029/06; **H04L-009/08** ; G06F-017/60
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 11042

English Abstract
An enterprise-based system includes a storage server equipped to generate a split encryption key having at least a first key portion and a second key portion, that is used by the storage server to encrypt at least a portion of a message. Additionally, the first key portion of the split encryption key is retained by the storage server, while the second key portion of the split encryption key is delivered to a message routing server and is discarded from the storage server. The message routing server in turn provides the second key portion to one or more recipients of the message to facilitate recipient access to the message.

French Abstract
L'invention concerne un systeme utilise dans le reseau d'une entreprise, comprenant un serveur de stockage concu pour produire une cle de chiffrement fractionnee comportant au moins une premiere partie et une seconde partie, utilisee par le serveur de stockage pour chiffrer au moins une partie d'un message. Par ailleurs, la premiere partie de la cle de chiffrement fractionnee est conservee par le serveur de stockage alors que la seconde partie de la cle de chiffrement fractionnee est fournie a un serveur de routage de messages et supprimee du serveur de stockage.

Legal Status (Type, Date, Text)
Publication 20040219 A1 With international search report.
Publication 20040219 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
...International Patent Class: **H04L-009/08**
Fulltext Availability:
Claims

Claim
... the second key portion.

12 In a storage server, a method comprising:
generating a split **encryption key** to **encrypt** a message, the split **encryption key** comprising at least a first **key portion** and a second **key portion** ;

generating a message **identifier** corresponding to the message;
I 0 generating one or more recipient-individualized tokens, each recipient...
? t22/5,k/22,24

22/5,K/22 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01006378 **Image available**
METHOD FOR BINDING A SOFTWARE DATA DOMAIN TO SPECIFIC HARDWARE
PROCEDE D'ASSOCIATION D'UN DOMAINE DES DONNEES LOGICIELLES A DU MATERIEL SPECIFIQUE

Patent Applicant/Assignee:
KONINKLIJKE PHILIPS ELECTRONICS N V, Groenewoudseweg 1, NL-5621 BA Eindhoven, NL, NL (Residence), NL (Nationality)
Inventor(s):
KRASINSKI Raymond, Prof. Holstlaan 6, NL-5656 AA Eindhoven, NL,
ROSNER Martin C, Prof. Holstlaan 6, NL-5656 AA Eindhoven, NL,
Legal Representative:
GROENENDAAL Antonius W M (agent), Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven, NL,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200336442 A2-A3 20030501 (WO 0336442)
Application: WO 2002IB4067 20021001 (PCT/WO IB02004067)
Priority Application: US 200143388 20011026
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
CN JP KR
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
Main International Patent Class: G06F-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 3397

English Abstract
A copy protection program (104) for securely holding digital audio and/or video content is bound to a particular device (100) via a key (200) derived in part (201) from unique or distinctive hardware, software and/or firmware identifiers within the device and in part (202) from a random or pseudo-random number. The key (200) is checked or rebuilt whenever the copy protection program (104) is employed to access protected digital content, either authorizing/prohibiting such access to the content or enabling/precluding proper decoding of the content. Therefore the digital content need not be directly bound to the device (100) while circumvention of the copy protection is frustrated.

French Abstract
La presente invention concerne un programme de protection contre la copie (104) permettant de conserver, de maniere sure, un contenu audio et/ou video numerique. Ledit programme est lie a un dispositif particulier (100) au moyen d'une cle (200) derivee dans la partie (201) d'identificateurs materiels, logiciels et/ou micrologiciels uniques ou distincts presents dans le dispositif et dans la partie (202) d'un nombre aleatoire ou pseudo-aleatoire. La cle (200) est verifiee ou reconstituee chaque fois que le programme de protection contre la copie (104) est utilise pour acceder au contenu numerique protege, autorisant/empechant

un tel acces au contenu ou permettant/interdisant le decodage approprie du contenu. Ainsi, le contenu numerique ne doit pas necessairement etre directement lie au dispositif (100) tant que le contournement de la protection contre la copie est neutralise.

Legal Status (Type, Date, Text)
Publication 20030501 A2 Without international search report and to be republished upon receipt of that report.
Search Rpt 20040318 Late publication of international search report
Republication 20040318 A3 With international search report.
Republication 20040318 A3 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Fulltext Availability:
Claims

Claim
... and the stored value relating to the key; and
employing the computed value for the **key** to **decrypt** the protected content.

3 The system as set forth in Claim 2 wherein the **key** is **derived** in **part** from a plurality of preselected unique or distinctive **identifiers** for hardware, software or firmware within the device.

4 The system as set forth in...

22/5,K/24 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00973626 **Image available**
ENCRYPTED COMMUNICATIONS SYSTEMS
SYSTEMES DE COMMUNICATION CRYPTES
Patent Applicant/Assignee:
SEPURA LIMITED, Radio House, St. Andrews Road, Cambridge CB4 1GR, GB, GB (Residence), GB (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
RAYNE Mark Wentworth, 5 St. James Close, Stretham, Nr Ely, Cambridgeshire CB6 3ND, GB, GB (Residence), GB (Nationality), (Designated only for: US)
Legal Representative:
FRANK B DEHN & CO (agent), 179 Queen Victoria Street, London EC4V 4EL, GB
,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200303648 A1 20030109 (WO 0303648)
Application: WO 2002GB2982 20020628 (PCT/WO GB0202982)
Priority Application: GB 200116016 20010629
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT (utility model) AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ (utility model) CZ DE (utility model) DE DK (utility model) DK DM DZ EC EE (utility model) EE ES FI (utility model) FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK (utility model) SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW

(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **H04L-009/18**
International Patent Class: **H04L-009/12**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 15128

English Abstract
In a communications system, transmission takes place in discrete time period bursts and a stream cipher algorithm is used to generate a key stream portion for encrypting information bits to be transmitted in a single transmission burst. The length of the key stream portion generated for encryption of the next transmission burst is adjust on the basis of the number of said information bits to be transmitted in the next transmission burst. Application to any communications system which produces a stream cipher, like, for example, GSM, TETRA, DECT, GPRS, EDGE and UMTS.

French Abstract
Dans un systeme de communication les transmissions s'effectuent par rafales dans des creneaux temporels discrets et on utilise un algorithme de cryptage en continu pour creer une portion de sequence de clefs de destinee a crypter des bits d'information en vue de leur transmission en une seule rafale de transmission. La longueur de la portion de la sequence de clefs servant a coder la prochaine rafale de transmission est modifiee en fonction du nombre de bits d'information contenus dans ladite prochaine rafale. Ce procede s'applique a tout systeme de communication utilisant le cryptage en continu tels que GSM, TETRA, DECT, GPRS, EDGE et UMTS.

Legal Status (Type, Date, Text)
Publication 20030109 A1 With international search report.
Publication 20030109 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

Main International Patent Class: **H04L-009/18**
International Patent Class: **H04L-009/12**
Fulltext Availability:
Detailed Description
Claims

Detailed Description
... or alter some other input value which is then combined with the initial input cryptographic **key** to generate the **encryption keys** to be used in the **key** stream **segment generating algorithm** (e.g. by repeating them in some order to form a suitable input **number**), and the **additional** , key-varying parameter could be ...incrementing or decrementing its value.

In a particularly preferred embodiment of the present invention, one **value** of the **additional** parameter (e.g. key segment number) is selected such that it will give the same **encryption key** for use in the **key** stream **segment generating algorithm** as would be the case when

no additional parameter is used in generating the **encryption key** (e.g. no additional parameter is combined with the common input key), i.e. the...any event). If more key stream segments are required for a given burst, then additional **encryption keys** and **key** stream **segments** can be **generated** by changing the **value** of the **additional** parameter as discussed above.

In the above aspects and embodiments of the present invention, it would be possible to vary only the **encryption key** used in the **key** stream segment generating algorithm to vary the key stream segments making up the key stream...be noted that in these arrangements, the initialisation vector repeat period for a given initial **encryption key** (i.e. the **key** supplied to the communication unit) is not altered (since although **additional** initialisation vector **values** are used for the additional **key** stream **segment** , that use is with different, **derived encryption keys** , not the initial **encryption key**). Thus each initial **encryption key** and initialisation vector combination still only occur once during the original lifetime of an initialisation...its value.

In a particularly preferred embodiment of the present invention, as for the multiple **encryption key** generation process, the multiple initialisation vector generation
- 27
process is preferably such that one **value** of the **additional** parameter (e.g. key segment number) can be (and is) selected such that it will give the same initialisation vector for use in the **key** stream **segment generating algorithm** as would be the case when no additional parameter is used in generating the initialisation...

...g. no additional parameter is combined with the initial initialisation vector).

Most preferably the same **value** of the **additional** parameter as gives an "unchanged" encryption **key** also gives an "unchanged" initialisation vector, as then in that case the same overall output **key** stream **segment** is **produced** as would be **produced** by equipment not using the additional parameter. This can allow backwards compatibility with existing equipment which does not generate additional **encryption keys** and/or initialisation vectors from the input key and initialisation vector, as by setting the additional parameter to this particular value, the **encryption key** stream **generator** will **generate** the same **key** stream **segment** as would be used by the existing equipment. The particular **additional** parameter **value** that does this ...key stream segments are required for a given burst, then additional initialisation vectors, and/or **encryption keys** , and **key** stream **segments** can be **generated** by changing the **value** of the **additional** parameter as discussed above.

As discussed above, the present invention is particularly, although not exclusively...produces further different

initialisation vectors, IVb and IVc. These additional initialisation vectors are used in **key** stream **segment generator** 2 together with their corresponding additional **encryption cipher keys** 9a (i.e. the **encryption cipher key** 9a **generated** using the same **key segment** number) to **generate** additional **key** stream **segments** KSSa, KSSb and KSSc which can, as discussed above, be appended to the basic **key** stream segment KSS to **encipher** or decipher longer (in terms of numbers of bits) transmission bursts.

Claim
... parameter is varied for each encryption key generated in such a way that generating an **encryption key** with each additional parameter value produces a different output **encryption key** .

16 The method of any one of claims 10 to 15, wherein one **value** of the **additional** parameter gives the same **encryption key** for use in the **key** stream **segment generating algorithm** as would be the case when no additional parameter is used in generating the **encryption key** .
17 The method of claim 16, comprising using the particular value of the additional parameter...the input key using an additional
parameter, wherein the additional parameter is varied for each **encryption key** generated in such a way that generating an **encryption key** with each **additional** parameter **value** produces a different output **encryption key** .

54 An apparatus for generating two or more initialisation vectors for use in a stream **cipher key** stream **segment generating algorithm** , the apparatus comprising:
means for **generating** each of the'two or more
- 57
initialisation vectors from an input initialisation vector using...
? t22/5,k/27,29

22/5,K/27 (Item 11 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00745762 **Image available**
MULTI-NODE ENCRYPTION AND KEY DELIVERY
CHIFFREMENT MULTINOEUD ET REMISE DE CLES
Patent Applicant/Assignee:
KONINKLIJKE PHILIPS ELECTRONICS N V, Groenewoudseweg 1, NL-5621 BA Eindhoven, NL, NL (Residence), NL (Nationality)
Inventor(s):
ROSNER Martin, Prof. Holstlaan 6, NL-5656 AA Eindhoven, NL
EPSTEIN Michael A, Prof. Holstlaan 6, NL-5656 AA Eindhoven, NL
PASIEKA Michael, Prof. Holstlaan 6, NL-5656 AA Eindhoven, NL
Legal Representative:
FAESSEN Louis M H, Internationaal Octrooibureau B.V., Prof. Holstlaan 6,

NL-5656 AA Eindhoven, NL
Patent and Priority Information (Country, Number, Date):
Patent: WO 200059154 A1 20001005 (WO 0059154)
Application: WO 2000EP1895 20000306 (PCT/WO EP0001895)
Priority Application: US 99126168 19990325; US 99434156 19991104
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
CN JP KR
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04L-009/08**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6441

English Abstract
The common encryption of content material is provided for decryption at a plurality of destination devices, each destination device having a unique private key of a public-private key pair. A multiple device key exchange is utilized to create a session key for encrypting the content material that is based on each of the public keys of the plurality of destination devices. The content material is encrypted using this session key. A partial key is also created for each of the intended destination devices that relies upon the private key of the destination device to form a decryption key that is suitable for decrypting the encrypted content material. The encrypted content material and the corresponding partial key are communicated to each destination device via potentially insecure means, including broadcast over a public network. Each destination device decrypts the encrypted content material using the decryption key that is formed from its private key and the received partial key. Including or excluding the public key of selected destination devices in the creation of the session key effects selective encryption.

French Abstract
L'invention concerne le chiffrement ordinaire d'un contenu destine au decryptage au niveau de plusieurs dispositifs destinataires, chaque dispositif possedant une cle privee unique d'une paire de cles privees-publiques. On utilise un echange de cles du dispositif multiple pour creer une cle de session permettant de chiffrer le contenu qui est fonde sur chacune des cles publiques de plusieurs dispositifs destinataires. Le contenu est chiffre a l'aide de cette cle de session. On cree egalement une cle partielle pour chacun des dispositifs destinataires souhaites qui depende de la cle privee du dispositif destinataire pour constituer une cle de decryptage appropriee au decryptage du contenu chiffre. Ce dernier et la cle partielle correspondante sont communiques a chaque dispositif destinataire par le biais d'un dispositif potentiellement non protege, y compris la diffusion sur un reseau publique. Chaque dispositif destinataire decrypte le contenu code a l'aide de la cle de decryptage qui est constituee a partir de sa cle privee et de la cle partielle recue. Inclure ou exclure la cle publique des dispositifs destinataires selectionnes lors de la creation de la cle de session agit sur le chiffrement selectif.

Legal Status (Type, Date, Text)
Publication 20001005 A1 With international search report.

Main International Patent Class: **H04L-009/08**
Fulltext Availability:

Detailed Description

Detailed Description
... Xy2 mod n, and so on.

Each destination device 250, 260, 270, 280 forms a **decryption key** 255, 265, 275, 285 by **forming** the product of its corresponding **partial key** 225, 226, 227, 228 and its **sub - key** 450, 460, 470, 480. As illustrated in FIG. 4, because each **sub key** Xy mod n is equivalent to Yx mod n (because (g')y mod n = (gy...

...encrypted content EK'(M) 53 1.

When each of the devices D1, D3, and D4 **form** the product of its **sub - key** and its **partial key** 525-528, the corresponding **decryption key** 555, 575, 585 is computed to be equal to (Y1 *Yz*Y3*Y4)x mod...

22/5,K/29 (Item 13 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00532355 **Image available**
METHOD OF CONTROLLING USAGE OF SOFTWARE COMPONENTS
PROCEDE DE COMMANDE D'UTILISATION DE COMPOSANTS LOGICIELS
Patent Applicant/Assignee:
INTEL CORPORATION,
KNAPTON Kenneth S III,
Inventor(s):
KNAPTON Kenneth S III,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9963707 A1 19991209
Application: WO 99US11106 19990519 (PCT/WO US9911106)
Priority Application: US 9892632 19980605
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class: **H04L-009/32**
Publication Language: English
Fulltext Availability:
Detailed Description
Cláims
Fulltext Word Count: 5402

English Abstract
Controlling the usage of a software component (16) by an application program (12) in an end user computer system (10) includes obtaining an identifier of the application program by a controller computer system (24) and generating a first password from the received application program identifier and an identifier of the component. The component, the component's identifier and the first password are communicated to the end user computer system. The component is registered with the application as a "snap-in" or "plug-in" component. The application program generates a second password from the application program identifier and the received

component identifier, compares the first password and the second password, and allows use of the "snap-in" component by the application program on te end user computer system when the first password matches the second password.

French Abstract

L'invention concerne la commande de l'utilisation d'un composant logiciel (16) par un programme d'application (12) dans un systeme informatique individuel (10), grace a l'obtention d'un identificateur du programme d'application par un systeme informatique de commande (24) et la generation d'un premier mot de passe a partir de l'identificateur de programme d'application recu et d'un identificateur du composant. Le composant, l'identificateur de composant et le premier mot de passe sont communiques au systeme informatique individuel. Le composant est enregistre avec le programme d'application comme composant "inserable" ou "enfichable". Le programme d'application genere un deuxieme mot de passe a partir de l'identificateur de programme d'application et de l'identificateur de composant recu, compare le premier mot de passe au deuxieme mot de passe, et autorise l'utilisation du composant "insere" par le programme d'application dans le systeme informatique individuel lorsque le premier mot de passe correspond au deuxieme mot de passe.

Main International Patent Class: **H04L-009/32**

Fulltext Availability:

Detailed Description

Claims

Detailed Description

... not restricted in scope in this respect.

At block 206, the controller security control operation **creates** an **encrypted component key** , using an unique **identifier** for the requested component and the secret **encryption key** as input data. As with generation of the application key, in one embodiment, the component **key** may be **encrypted** according to the well known DES technique, although other encryption techniques may also be employed...

...of the present invention. The application license number 230 provided by the end user is **encrypted** using the secret **encryption key** 232 to **produce** application **key** 234. Similarly, component identifier (ID) 236 is **encrypted** with the secret **encryption key** 232 to produce component **key** 238. The application key and the **component key** are then **encrypted** with the secret **encryption key** to produce the component password 240. In another embodiment, different **encryption keys** may be used to generate the application key, the component key, and the component password...

Claim

... 5, wherein generating the second password comprises:

creating a first key from the application program **identifier** ;

creating a second **key** from the received **component identifier** ; and

creating the second password from the first and second keys.

7 The method of claim 6, wherein creating the first **key** comprises **encrypting** at least a portion of the application program identifier with a secret encryption key.

8...13, wherein generating the first password comprises:

creatinv a first key from the application program **identifier** ;

creatin a second **key** from the **component identifier** ; and

9

creating the first password from the first and second keys.

16 The method of claim 15, wherein creating the first **key** comprises **encrypting** at least a portion of the application program identifier with a secret encryption key.

17...
...creating the first password comprises
encrypting a combination of the first key and the second **key** with a secret **encryption key** .

19 The method of claim 14, wherein generating the second password comprises:
creating a third key from the application program **identifier** ;
creating a fourth **key** from the communicated **component identifier** ; and
creating the second password from the third and fourth keys.

20 The method of claim 19, wherein creating the third **key** comprises **encrypting** at least a portion of the application program identifier with a secret encryption key.

```
File 347:JAPIO Nov 1976-2004/Aug(Updated 041203)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200481
         (c) 2004  Thomson Derwent

Set     Items   Description
S1     374561   CODE OR CODES OR CODED OR CODING? ? OR SUBCOD???? ?
S2    2843699   NUMBER? ? OR NUMERAL? ? OR NUMERIC?? ? OR ALPHANUMERIC? OR
            INTEGER? ? OR DIGIT? ? OR VALUE OR VALUES
S3    1104665   SEQUENCE? OR SEQUENT? OR BIT OR BITS OR SUBSEQUEN? OR STRI-
            NG? ? OR STRINGS
S4    1105717   POINT? OR IDENTIFIER? ? OR SUBKEY? ? OR SUB()KEY? ?
S5       9610   (S1:S3 OR MICROCOD???? ?)(3N)ADDITIONAL
S6      18773   (S1:S3 OR MICROCOD???? ?)(3N)(AUXILAR? OR AUXILIAR? OR AUX-
            ILL? OR ADJUNCT? OR ANCILLAR? OR ANCILLIA? OR SUPPLEMENT? OR -
            INDEX??? ?)
S7     261725   KEY? ? OR CIPHER? ? OR CYPHER? ? OR ALGORITHM? OR KEYPAIR?
S8      25652   S7(3N)(PARTIAL? OR PORTION? ? OR FRAGMENT? OR SECTION? OR -
            PARTITION? OR PIECE? ? OR PART OR PARTS OR COMPONENT? OR SUBC-
            OMPONENT?)
S9        773   S7(3N)(SUBSET? OR SUB()SET? ? OR SEGMENT? OR FRACTION?)
S10      1324   S8:S9(5N)(GENERAT? OR DERIV??? ? OR DERIVAT? OR PRODUCE? ?
            OR PRODUCING OR PRODUCTION? ? OR PROD? ? OR CREAT???? ? OR CO-
            NSTRUCT?)
S11      1666   S8:S9(5N)(FORM OR FORMS OR FORMED OR FORMING OR FORMATION?
            ? OR SYNTHESIS? OR SYNTHESIZ? OR ORIGINAT? OR DEVELOP?)
S12       198   S10:S11 AND S4:S6
S13     13753   S7(5N)(ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR DECOD???? ? OR
             ENCOD???? ? OR INCOD???? ? OR UNENCOD? OR UNINCOD? OR DECRYP-
            T?)
S14      1119   S7(5N)(UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR DECIPHE-
            R? OR DECYPHER? OR UNCRYPT? OR UNCIPHER? OR UNCYPHER? OR UNCO-
            D???? ?)
S15        17   S12 AND S13:S14
S16        17   IDPAT (sorted in duplicate/non-duplicate order)
S17        17   IDPAT (primary/non-duplicate records only)
?
```

? t17/9/2,5,8

17/9/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014804214 **Image available**
WPI Acc No: 2002-624920/200267
Method and apparatus for encoding and decoding **file using basic and disposable** keys
Patent Assignee: NITZ CORP (NITZ-N)
Inventor: YANG T Y
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2002025343	A	20020404	KR 200057063	A	20000928	200267	B

Priority Applications (No Type Date): KR 200057063 A 20000928
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2002025343	A		1	G09C-001/00	

Abstract (Basic): KR 2002025343 A
NOVELTY - A method and apparatus for encoding and **decoding** file using basic and disposable **keys** are provided to generate and **encode** a password **key** based on basic and disposable keys and form information having the disposable key as a header.
DETAILED DESCRIPTION - A basic **key generation** storage **section** (501) **generates** an initial key based on a user' input information and time information of an **encoding** system. The basic **key generation** storage **section** (501) **generates** a random number having the initial key as a seed. The basic **key generation** storage **section** (501) stores the random number as a basic key. A disposable key generator(507) receives time information of a time **point** when a plaintext file is encoded, drives a random number generator using the data as a seed, and outputs a resulting disposable key. A password key generator(503) generates a password key based on the basic and disposable **keys** . A first **encoder** (505) receives the password **key** , **encodes** a plaintext file, and outputs encoded data. A second encoder(509) sets the encoded data as a password file body, sets information having the disposable key as a password file header, and outputs a final encoded file.
pp; 1 DwgNo 1/10
Title Terms: METHOD; APPARATUS; ENCODE; DECODE; FILE; BASIC; DISPOSABLE; KEY
Derwent Class: P85
International Patent Class (Main): G09C-001/00
File Segment: EngPI

17/9/5 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011377543 **Image available**
WPI Acc No: 1997-355450/199733
XRPX Acc No: N97-294785
Individual authentication system for cash transaction service system in bank - compares decoded finger print information with predetermined

information that is not enciphered and if both are in agreement, it is judged that individual authentication is carried out
Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)
Number of Countries: 001 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 9147072	A	19970606	JP 95326467	A	19951121	199733	B
JP 3564673	B2	20040915	JP 95326467	A	19951121	200460	

Priority Applications (No Type Date): JP 95326467 A 19951121
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 9147072	A		6	G06K-017/00	
JP 3564673	B2		8	G06K-017/00	Previous Publ. patent JP 9147072

Abstract (Basic): JP 9147072 A
The system includes an individual authentication card which has a finger print reader (11) and an **encryptment key formation part** (12). The **encryptment key formation part** provides an **encrypted key** according to the combination of the finger **point** information read by finger print reader and the attribute of the individual authentication card. A predetermined information is enciphered using an encipherment part (14). A terminal equipment (20) has a signal sending out unit to send out the ID of the user corresponding to the read finger print.
An open key management system stores the open key according to the user ID received from the terminal equipment. A decoder decodes the encrypted predetermined information. A communication network transmits the predetermined information that is not enciphered and this information is compared with the output of the decoder and if both are in agreement, it is judged that the individual authentication is carried out.
ADVANTAGE - Prevents risk of being robbed of finger print information.
Dwg.1/2
Title Terms: INDIVIDUAL; AUTHENTICITY; SYSTEM; CASH; TRANSACTION; SERVICE; SYSTEM; BANK; COMPARE; DECODE; FINGER; PRINT; INFORMATION; PREDETERMINED; INFORMATION; ENCIPHER; AGREE; JUDGEMENT; INDIVIDUAL; AUTHENTICITY; CARRY
Derwent Class: P31; S05; T01; T04; T05
International Patent Class (Main): G06K-017/00
International Patent Class (Additional): A61B-005/117; G06K-019/10; G06T-007/00
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): S05-D01C5A; T01-D01; T01-H01C1; T01-J10B2; T01-J12C ; T04-C; T04-D04; T05-D01B; T05-L03C

17/9/8 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX

007654091 **Image available**
WPI Acc No: 1988-288023/198841
XRPX Acc No: N88-218580
Personal computer with encrypted programs - has microprocessor determining which encryption key **to fetch from read only store and uses** key **to** decode **program**
Patent Assignee: IBM CORP (IBMC)
Inventor: BUURMAN L L
Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
GB 2203271	A	19881012	GB 877850	A	19870402	198841	B

Priority Applications (No Type Date): GB 877850 A 19870402
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
GB 2203271	A		12		

Abstract (Basic): GB 2203271 A

A microprocessor operates under control of a read only store and code stored in random access memory. The microprocessor receives programs in encrypted form and from a program imbedded **encryption key identifier** or **identifiers** determine which **encryption key** or **keys** to fetch from the read only store and subsequently uses the fetched **key** or **keys** to **decode** . The latter involves the received encoded/encrypted program being decrypted to load a decoded/decrypted code into the random access memory for subsequent execution.

One or more keys may be reserved for use with unencrypted programs. The read only store contains a table containing the **encryption keys** . The microprocessor **forms part** of an adaptor by which an input/output device may be connected to a system bus.

ADVANTAGE - Prevents unauthorised copying of programs.

1/6

Title Terms: PERSON; COMPUTER; ENCRYPTION; PROGRAM; MICROPROCESSOR; DETERMINE; ENCRYPTION; KEY; FETCH; READ; STORAGE; KEY; DECODE; PROGRAM
Derwent Class: T01
International Patent Class (Additional): G06F-012/14
File Segment: EPI
Manual Codes (EPI/S-X): T01-H01B; T01-H01C
? t17/9/9,11

17/9/9 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

002392643
WPI Acc No: 1980-K9113C/198045
Portable electronic cryptographic device - has keyboard and display with circuitry which can encipher and decipher **plain text using randomised message** key
Patent Assignee: DATOTEK INC (DATO-N)
Inventor: CARTER M B; MORGAN B O
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 4229817	A	19801021				198045	B

Priority Applications (No Type Date): US 78901068 A 19780428

Abstract (Basic): US 4229817 A

The device incorporates a random code generator for generating a randomised message key which, together with the keyboard inputs, initiates and generates a long sequence of randomised letters for enciphering purposes. In a **deciphering** mode, a predetermined message **key** may be entered to set the random code generator at a **point** to generate the originally entered plain text.

A basic **key** composed of multiple **segments** fully initialises the random code **generator** such that more than one device could be used to encipher and decipher text. By using different segments of the basic

key, varying levels of security can be obtained. Test circuitry is provided to insure maintenance of the proper key variables and proper operation of the device.

Title Terms: PORTABLE; ELECTRONIC; CRYPTOGRAPHIC; DEVICE; KEYBOARD; DISPLAY ; CIRCUIT; CAN; ENCIPHER; DECIPHER; PLAIN; TEXT; RANDOM; MESSAGE; KEY
Derwent Class: W01; W02
International Patent Class (Additional): H04K-001/02; H04L-009/00
File Segment: EPI
Manual Codes (EPI/S-X): W01-A05; W02-L

17/9/11 (Item 11 from file: 347)
DIALOG(R)File 347:JAPIO

07715641 **Image available**
CONTENT PROTECTIVE STORAGE DEVICE, TERMINAL EQUIPMENT, AND CONTENT PROTECTIVE SYSTEM

PUB. NO.: 2003-209541 [JP 2003209541 A]
PUBLISHED: July 25, 2003 (20030725)
INVENTOR(s): HATTORI TAKEHIRO
SATO KENSUKE
APPLICANT(s): MATSUSHITA ELECTRIC IND CO LTD
APPL. NO.: 2002-003120 [JP 20023120]
FILED: January 10, 2002 (20020110)
INTL CLASS: H04L-009/08; G06F-015/00; G06F-017/60; H04L-009/10

ABSTRACT

PROBLEM TO BE SOLVED: To give a permission to browse contents from the outside of an information terminal and to protect the contents.

SOLUTION: The contents stored in a storage device are transferred to the information terminal 20, and when a user browses them, the information terminal 20 ciphers the contents by a cipher key different at each time and reads them. The information terminal 20 requests a **decipher key** corresponding to the **identifier** of the cipher key to a telephone corresponding machine 30. A deciphering part 21 performs **deciphering** by using the decipher **key** notified from the **decipher key generation part** 31 of the telephone corresponding machine 30 and outputs the contents to the user.

? t17/9/16-17

17/9/16 (Item 16 from file: 347)
DIALOG(R)File 347:JAPIO

05917661 **Image available**
CIPHER COMMUNICATING METHOD FOR FACSIMILE EQUIPMENT

PUB. NO.: 10-200761 [JP 10200761 A]
PUBLISHED: July 31, 1998 (19980731)
INVENTOR(s): SHIBATA KOICHI
APPLICANT(s): MITA IND CO LTD [000615] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 09-003733 [JP 973733]
FILED: January 13, 1997 (19970113)
INTL CLASS: [6] H04N-001/44

JAPIO CLASS: 29.4 (PRECISION INSTRUMENTS -- Business Machines); 44.7 (COMMUNICATION -- Facsimile)
JAPIO KEYWORD: R131 (INFORMATION PROCESSING -- Microcomputers & Microprocessers)

ABSTRACT

PROBLEM TO BE SOLVED: To provide the cipher communicating method of a facsimile equipment, in which a **cipher** sentence is difficult to be **decoded** by a third person, by using a self-synchronous stream ciphering method.

SOLUTION: When a reception-side facsimile equipment is provided with a cipher communication function, cipher communication is possible and therefore a transmission-side facsimile equipment selects the **index number** of an **index** for initial **value** selection and the **index number** of an **index** for register selection, which are stored in a storage part 4, based on a communication date from a date data generation part 2. Then, data encoded in an encoding part 15 is ciphered by using a cipher key system **generated** in a **cipher key** system **generation part** 3 and the **cipher** sentence is **generated** . When cipher communication is sent from the transmission-side facsimile equipment, the reception-side facsimile equipment similarly selects the **index number** of the **index** for initial **value** selection and the **index number** of the **index** for register selection based on the communication date. Then, the cipher sentence is made into a normal sentence based on the cipher key system generated in the generation part 3.

17/9/17 (Item 17 from file: 347)

04544997 **Image available**
DATA TRANSMITTER-RECEIVER

PUB. NO.: 06-216897 [JP 6216897 A]
PUBLISHED: August 05, 1994 (19940805)
INVENTOR(s): AOYANAGI HIDEYUKI
APPLICANT(s): NIPPON SIGNAL CO LTD THE [000465] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 05-024750 [JP 9324750]
FILED: January 20, 1993 (19930120)
INTL CLASS: [5] H04L-009/06; H04L-009/14; G09C-001/00
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.9 (COMMUNICATION -- Other)
JOURNAL: Section: E, Section No. 1626, Vol. 18, No. 580, Pg. 30, November 07, 1994 (19941107)

ABSTRACT

PURPOSE: To allow the transmitter-receiver to cope with a fact that the strength of ciphering is high and a common **key** might be **decoded** by storing plural common **key** data in advance and revising the common key under a prescribed condition.

CONSTITUTION: A sender side is provided with a **key generating section** 1 **generating** plural kinds of **sub keys** based on a prescribed common key K(sub 1). The common key K(sub 1) fed to the **key generating section** 1 is selected alternatively by a key data selection section 2 from plural common keys K(sub 1)-K(sub n) stored in advance in a memory of a transmission side and a data random section 3 uses **sub keys** K(sub

1).K(sub 1)-K(sub 1).K(sub n) of the **key generating section** 1 to **generate** a ciphered sentence K/D according to a prescribed algorithm from transmission data D. A **key** data **generating section** 11 on a receiver side **generates** plural kinds of **sub keys** K(sub 1).K(sub 1)-K(sub 1).K(sub n) based on the common key K(sub 1) and a data random section 13 decodes the ciphered sentence K.D received from a reception section 15 according to a prescribed algorithm. The key data selection section 2 on the sender side selects a common key under a certain condition such as that after lapse of prescribed time.
?

```
File   6:NTIS 1964-2004/Dec W1
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
File   2:INSPEC 1969-2004/Dec W2
         (c) 2004 Institution of Electrical Engineers
File   8:Ei Compendex(R) 1970-2004/Dec W2
         (c) 2004 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2004/Dec W2
         (c) 2004 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2004/Dec
         (c) 2004 ProQuest Info&Learning
File  65:Inside Conferences 1993-2004/Dec W3
         (c) 2004 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2004/Nov W2
         (c)2004 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2004/Jun W1
         (c) 2004 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Nov
         (c) 2004 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2004/Dec 16
         (c) 2004 The Gale Group
File 144:Pascal 1973-2004/Dec W1
         (c) 2004 INIST/CNRS
File 202:Info. Sci. & Tech. Abs. 1966-2004/Nov 02
         (c) 2004 EBSCO Publishing
File 233:Internet & Personal Comp. Abs. 1981-2003/Sep
         (c) 2003 EBSCO Pub.
File 256:TecInfoSource 82-2004/Nov
         (c) 2004 Info.Sources Inc
File 266:FEDRIP 2004/Sep
         Comp & dist by NTIS, Intl Copyright All Rights Res
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File 483:Newspaper Abs Daily 1986-2004/Dec 18
         (c) 2004 ProQuest Info&Learning
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 603:Newspaper Abstracts 1984-1988
         (c)2001 ProQuest Info&Learning

Set     Items   Description
S1    1112532   CODE OR CODES OR CODED OR CODING? ? OR SUBCOD???? ?
S2    8734498   NUMBER? ? OR NUMERAL? ? OR NUMERIC?? ? OR ALPHANUMERIC? OR
            INTEGER? ? OR DIGIT? ? OR VALUE OR VALUES
S3    3094843   SEQUENCE? OR SEQUENT? OR BIT OR BITS OR SUBSEQUEN? OR STRI-
            NG? ? OR STRINGS
S4    2971116   POINT? OR IDENTIFIER? ? OR SUBKEY? ? OR SUB()KEY? ?
S5      22105   (S1:S3 OR MICROCOD???? ?)(3N)ADDITIONAL
S6      72370   (S1:S3 OR MICROCOD???? ?)(3N)(AUXILAR? OR AUXILIAR? OR AUX-
            ILL? OR ADJUNCT? OR ANCILLAR? OR ANCILLIA? OR SUPPLEMENT? OR -
            INDEX??? ?)
S7    2769814   KEY? ? OR CIPHER? ? OR CYPHER? ? OR ALGORITHM? OR KEYPAIR?
S8      78351   S7(3N)(PARTIAL? OR PORTION? ? OR FRAGMENT? OR SECTION? OR -
            PARTITION? OR PIECE? ? OR PART OR PARTS OR COMPONENT? OR SUBC-
            OMPONENT?)
S9      24897   S7(3N)(SUBSET? OR SUB()SET? ? OR SEGMENT? OR FRACTION?)
S10      4824   S8:S9(5N)(GENERAT? OR DERIV??? ? OR DERIVAT? OR PRODUCE? ?
            OR PRODUCING OR PRODUCTION? ? OR PROD? ? OR CREAT???? ? OR CO-
            NSTRUCT?)
S11      6598   S8:S9(5N)(FORM OR FORMS OR FORMED OR FORMING OR FORMATION?
            ? OR SYNTHESIS? OR SYNTHESIZ? OR ORIGINAT? OR DEVELOP?)
S12     35716   S7(5N)(ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR DECOD???? ? OR
```

ENCOD???? ? OR INCOD???? ? OR UNENCOD? OR UNINCOD? OR DECRYP-
T?)
S13 431 S7(5N)(UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR DECIPHE-
R? OR DECYPHER? OR UNCRYPT? OR UNCIPHER? OR UNCYPHER? OR UNCO-
D???? ?)
S14 917 S10:S11 AND S4:S6
S15 32 S14 AND (ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR DECOD???? ?
OR ENCOD???? ? OR INCOD???? ? OR UNENCOD? OR UNINCOD? OR DECR-
YPT?)
S16 2 S14 AND (UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR DECIP-
HER? OR DECYPHER? OR UNCRYPT? OR UNCIPHER? OR UNCYPHER? OR UN-
COD???? ?)
S17 33 S15:S16
S18 11 S17/2000:2004
S19 22 S17 NOT S18
S20 14 RD (unique items)

20/7/11 (Item 3 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

913063 ORDER NO: AAD86-07767
INTEGRATING HIERARCHICALLY SIGNIFICANT PART NUMBERS TO BILL OF MATERIALS PROCESSING (DATA STRUCTURES)
Author: KINI, RANJAN BAILUR
Degree: D.B.A.
Year: 1985
Corporate Source/Institution: TEXAS TECH UNIVERSITY (0230)
Source: VOLUME 47/02-A OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 573. 128 PAGES

The Bill of Materials is the front-end information required in the material planning function of an organization. Processing of the Bills of Materials in an organization is usually computerized. Products can be exploded and requirements for the production schedule can be planned in an efficient and timely manner. Currently, bill processing is performed by maintaining two separate direct access files--Item Master File and Product Structure File. By linking these two files through **pointers** , product explosion or implosion is accomplished. This method, since it incurs a large number of disk accesses, slows down Master Production Schedule explosion in material planning. Most major commerical software are using basically the same logic in their bill processing applications.

Although part numbers are not related to bill processing other than to uniquely identify a part, a new part numbering scheme indicated an opportunity to use it in bill processing. This Hierarchically Significant Part Numbering (HSPN) scheme through its unique **encoding / decoding part** numbering **algorithm generates** a numerator/denominator part number embedding the parent-child linkage information in it.

This information about the structure is used in developing the HSPN approach to bill processing. This approach not only identifies a part uniquely but also helps out substantially in the data processing function of bill processing by exploding and imploding a product much faster.

The HSPN approach is compared to the current link listing approach for its performance in explosion/implosion queries. The testing is conducted by simulating both the approaches and actually counting instruction operations for each query. For data, a set of complex product structures used in several other research is used.

The results have indicated the HSPN approach to be far superior to the current link listing approach. When the tables of part numbers used in the HSPN approach are kept in entirety in the main memory the HSPN approach performed significantly better by a factor of 150 in all explosion and

implosion queries; whereas, when only the partial segments of tables are brought into the main memory the HSPN performed moderately better than the current approach. Regardless, the HSPN approach has shown a new way of processing the bills and an approach to process the bill significantly faster than with the traditional approach.

20/7/12 (Item 1 from file: 94)

02029303 JICST ACCESSION NUMBER: 94A0324513 FILE SEGMENT: JICST-E

Improved cryptograph based on Vernam cipher.

OMAE YOSHITSUGU (1); TAKAHASHI SADAYOSHI (1); OTAKI KATSUHISA (2)
(1) Kanagawakokadai; (2) Seibuhyakkaten

Kanagawa Koka Daigaku Kenkyu Hokoku. B. Rikogakuhen(Research Reports of Kanagawa Institute of Technology. Part B. Science and Technology), 1994, NO.18, PAGE.179-187, FIG.4, TBL.5, REF.8
JOURNAL NUMBER: S0956ABN ISSN NO: 0916-1902
UNIVERSAL DECIMAL CLASSIFICATION: 681.3.01 681.3.02-759 621.391.037.3
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication

ABSTRACT: In this paper, traditional Vernam cipher is investigated and the improved cryptograph having a procedure-open-type algorithm with a new mixing function in the **key generation part** of the Vernam **cipher** is proposed. The main improvement **point** is to generate a non-periodic long random sequence and to attain the high security, by using the AMIDA lottery structure for the part of generation on the key stream of the Vernam cipher. In this method, the entrance of the AMIDA structure and also the random seed of the random sequence generator situated at the exit of the AMIDA structure, are changed after each one block **encipher** (**decipher**). (author abst.)

```
File 696:DIALOG Telecom. Newsletters 1995-2004/Dec 18
         (c) 2004 The Dialog Corp.
File  15:ABI/Inform(R) 1971-2004/Dec 20
         (c) 2004 ProQuest Info&Learning
File  98:General Sci Abs/Full-Text 1984-2004/Sep
         (c) 2004 The HW Wilson Co.
File 112:UBM Industry News 1998-2004/Jan 27
         (c) 2004 United Business Media
File 141:Readers Guide 1983-2004/Sep
         (c) 2004 The HW Wilson Co
File 484:Periodical Abs Plustext 1986-2004/Dec W2
         (c) 2004 ProQuest
File 608:KR/T Bus.News. 1992-2004/Dec 20
         (c)2004 Knight Ridder/Tribune Bus News
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2004/Dec 20
         (c) 2004 PR Newswire Association Inc
File 635:Business Dateline(R) 1985-2004/Dec 18
         (c) 2004 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 610:Business Wire 1999-2004/Dec 13
         (c) 2004 Business Wire.
File 369:New Scientist 1994-2004/Dec W1
         (c) 2004 Reed Business Information Ltd.
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File  20:Dialog Global Reporter 1997-2004/Dec 20
         (c) 2004 The Dialog Corp.
File 624:McGraw-Hill Publications 1985-2004/Dec 20
         (c) 2004 McGraw-Hill Co. Inc
File 634:San Jose Mercury  Jun 1985-2004/Dec 16
         (c) 2004 San Jose Mercury News
File 647:CMP  Computer Fulltext 1988-2004/Dec W2
         (c) 2004 CMP Media, LLC
File 674:Computer News Fulltext 1989-2004/Dec W1
         (c) 2004 IDG Communications

Set     Items   Description
S1    1492712   CODE OR CODES OR CODED OR CODING? ? OR SUBCOD???? ?
S2   12237760   NUMBER? ? OR NUMERAL? ? OR NUMERIC?? ? OR ALPHANUMERIC? OR
             INTEGER? ? OR DIGIT? ? OR VALUE OR VALUES
S3    3328179   SEQUENCE? OR SEQUENT? OR BIT OR BITS OR SUBSEQUEN? OR STRI-
             NG? ? OR STRINGS
S4    7025189   POINT? OR IDENTIFIER? ? OR SUBKEY? ? OR SUB()KEY? ?
S5      64831   (S1:S3 OR MICROCOD???? ?)(3N)ADDITIONAL
S6      51184   (S1:S3 OR MICROCOD???? ?)(3N)(AUXILAR? OR AUXILIAR? OR AUX-
             ILL? OR ADJUNCT? OR ANCILLAR? OR ANCILLIA? OR SUPPLEMENT? OR -
             INDEX??? ?)
S7    4203562   KEY? ? OR CIPHER? ? OR CYPHER? ? OR ALGORITHM? OR KEYPAIR?
S8     197415   S7(3N)(PARTIAL? OR PORTION? ? OR FRAGMENT? OR SECTION? OR -
             PARTITION? OR PIECE? ? OR PART OR PARTS OR COMPONENT? OR SUBC-
             OMPONENT?)
S9      17543   S7(3N)(SUBSET? OR SUB()SET? ? OR SEGMENT? OR FRACTION?)
S10      6874   S8:S9(5N)(GENERAT? OR DERIV??? ? OR DERIVAT? OR PRODUCE? ?
             OR PRODUCING OR PRODUCTION? ? OR PROD? ? OR CREAT???? ? OR CO-
             NSTRUCT?)
S11     10817   S8:S9(5N)(FORM OR FORMS OR FORMED OR FORMING OR FORMATION?
             ? OR SYNTHESIS? OR SYNTHESIZ? OR ORIGINAT? OR DEVELOP?)
S12     23897   S7(5N)(ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR DECOD???? ? OR
```

```
            ENCOD???? ? OR INCOD???? ? OR UNENCOD? OR UNINCOD? OR DECRYP-
            T?)
S13       721   S7(5N)(UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR DECIPHE-
            R? OR DECYPHER? OR UNCRYPT? OR UNCIPHER? OR UNCYPHER? OR UNCO-
            D???? ?)
S14       640   S10:S11(S)S4:S6
S15        16   S14(S)(ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR DECOD???? ? OR
            ENCOD???? ? OR INCOD???? ? OR UNENCOD? OR UNINCOD? OR DECRYP-
            T?)
S16         1   S14(S)(UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR DECIPHE-
            R? OR DECYPHER? OR UNCRYPT? OR UNCIPHER? OR UNCYPHER? OR UNCO-
            D???? ?)
S17        17   S15:S16
S18         9   S17/2000:2004
S19         8   S17 NOT S18
S20         7   RD (unique items)
?
```

```
File   9:Business & Industry(R) Jul/1994-2004/Dec 17
         (c) 2004  The Gale Group
File  13:BAMP 2004/Dec W2
         (c) 2004  The Gale Group
File  16:Gale Group PROMT(R) 1990-2004/Dec 20
         (c) 2004 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2004/Dec 20
         (c) 2004 The Gale group
File 148:Gale Group Trade & Industry DB 1976-2004/Dec 20
         (c)2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2004/Dec 20
         (c) 2004 The Gale Group
File 570:Gale Group MARS(R) 1984-2004/Dec 20
         (c) 2004 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2004/Dec 20
         (c) 2004 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2004/Dec 20
         (c) 2004 The Gale Group
File 649:Gale Group Newswire ASAP(TM) 2004/Dec 13
         (c) 2004 The Gale Group

Set     Items   Description
S1    1474297   CODE OR CODES OR CODED OR CODING? ? OR SUBCOD???? ?
S2   10504560   NUMBER? ? OR NUMERAL? ? OR NUMERIC?? ? OR ALPHANUMERIC? OR
              INTEGER? ? OR DIGIT? ? OR VALUE OR VALUES
S3    2410352   SEQUENCE? OR SEQUENT? OR BIT OR BITS OR SUBSEQUEN? OR STRI-
              NG? ? OR STRINGS
S4    4688502   POINT? OR IDENTIFIER? ? OR SUBKEY? ? OR SUB()KEY? ?
S5      81161   (S1:S3 OR MICROCOD???? ?)(3N)ADDITIONAL
S6      51608   (S1:S3 OR MICROCOD???? ?)(3N)(AUXILAR? OR AUXILIAR? OR AUX-
              ILL? OR ADJUNCT? OR ANCILLAR? OR ANCILLIA? OR SUPPLEMENT? OR -
              INDEX??? ?)
S7    4191933   KEY? ? OR CIPHER? ? OR CYPHER? ? OR ALGORITHM? OR KEYPAIR?
S8     225977   S7(3N)(PARTIAL? OR PORTION? ? OR FRAGMENT? OR SECTION? OR -
              PARTITION? OR PIECE? ? OR PART OR PARTS OR COMPONENT? OR SUBC-
              OMPONENT?)
S9      25671   S7(3N)(SUBSET? OR SUB()SET? ? OR SEGMENT? OR FRACTION?)
S10      8928   S8:S9(5N)(GENERAT? OR DERIV??? ? OR DERIVAT? OR PRODUCE? ?
              OR PRODUCING OR PRODUCTION? ? OR PROD? ? OR CREAT???? ? OR CO-
              NSTRUCT?)
S11     12391   S8:S9(5N)(FORM OR FORMS OR FORMED OR FORMING OR FORMATION?
              ? OR SYNTHESIS? OR SYNTHESIZ? OR ORIGINAT? OR DEVELOP?)
S12     43946   S7(5N)(ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR DECOD???? ? OR
               ENCOD???? ? OR INCOD???? ? OR UNENCOD? OR UNINCOD? OR DECRYP-
              T?)
S13       847   S7(5N)(UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR DECIPHE-
              R? OR DECYPHER? OR UNCRYPT? OR UNCIPHER? OR UNCYPHER? OR UNCO-
              D???? ?)
S14       573   S10:S11(S)S4:S6
S15         9   S14(S)S12:S13
S16        14   S14(S)(ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR DECOD???? ? OR
               ENCOD???? ? OR INCOD???? ? OR UNENCOD? OR UNINCOD? OR DECRYP-
              T?)
S17         1   S14(S)(UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR DECIPHE-
              R? OR DECYPHER? OR UNCRYPT? OR UNCIPHER? OR UNCYPHER? OR UNCO-
              D???? ?)
S18        15   S15:S17
S19         0   S18/2000:2004
```

```
S20          15   S18 NOT S19
S21           8   RD (unique items)
?
```

File 347:JAPIO Nov 1976-2004/Aug(Updated 041203)
(c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200481
(c) 2004 Thomson Derwent
File 348:EUROPEAN PATENTS 1978-2004/Dec W02
(c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20041216,UT=20041209
(c) 2004 WIPO/Univentio

Set	Items	Description
S1	7047	AU=FUJII Y?
S2	88	AU=FUJI Y?
S3	1	AU=SHINZAKI Y?
S4	132	AU=TAKASHI S?
S5	0	AU=YUSAKU F?
S6	558151	ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR DECOD???? ? OR ENCOD-???? ? OR INCOD???? ? OR UNENCOD? OR UNINCOD? OR DECRYPT? OR -UNENCRYPT?
S7	10863	UNENCIPHER? OR UNENCYPHER? OR DECIPHER? OR DECYPHER? OR UN-CRYPT? OR UNCOD???? ? OR UNCIPHER? OR UNCYPHER?
S8	5750	S6:S7(5N)(PHYSICAL OR BIOMETR? OR FINGERPRINT? OR PRINT? ?)
S9	7257	S1:S4
S10	2	S9 AND S8

10/5/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01267574
Authentication device using anatomical information and method thereof
Beglaubigungsvorrichtung and Verfahren, die anatomische Informationen verwenden
Dispositif d'authentification utilisant des informations anatomiques et son procede d'utilisation
PATENT ASSIGNEE:
FUJITSU LIMITED, (211463), 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP), (Applicant designated States: all)
INVENTOR:
Ikegami, Jun, c/o Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki, Kanagawa 211-8588, (JP)
Shinzaki, Takashi, c/o Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki, Kanagawa 211-8588, (JP)
Fujii, Yusaka , c/o Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki, Kanagawa 211-8588, (JP
LEGAL REPRESENTATIVE:
Mohun, Stephen John (76153), Haseltine Lake & Co., Imperial House, 15-19 Kingsway, London WC2B 6UD, (GB)
PATENT (CC, No, Kind, Date): EP 1093045 A1 010418 (Basic)
APPLICATION (CC, No, Date): EP 306908 000814;
PRIORITY (CC, No, Date): JP 99293543 991015
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G06F-001/00; G07C-009/00

ABSTRACT EP 1093045 A1
An authentication device method and program collates and preferably encrypts information for authentication.
Collation information comprises anatomical information, such as finger print feature information, etc., and identification information. For the identification information, the serial number or equipment description of

a device by which the anatomical information is collected, information about a route taken between a collection device and an authentication device or serial number attached to anatomical information collected by a specifying device, etc., may be used instead of conventional time information. Then, the entire collation information is encrypted and is transmitted from an anatomical information collecting device to an authentication device via a network.

ABSTRACT WORD COUNT: 106

NOTE:
Figure number on first page: 10 8

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 010418 A1 Published application with search report
Examination: 010516 A1 Date of request for examination: 20010319
Examination: 030319 A1 Date of dispatch of the first examination report: 20030129

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200116	1258
SPEC A	(English)	200116	8359
Total word count - document A			9617
Total word count - document B			0
Total word count - documents A + B			9617

10/5/2 (Item 2 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01225663

Methods and equipment for encrypting/decrypting, and indentification systems

Verfahren und Vorrichtung zur Verschlusselung/entschlusselung sowie Identifikationssysteme

Procedes et dispositif de chiffrage/dechiffrage et systemes d'identification

PATENT ASSIGNEE:
FUJITSU LIMITED, (211463), 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP), (Applicant designated States: all)

INVENTOR:
Fujii, Yusaku c/o Fujitsu Limited , 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
Shinzaki, Takashi c/o Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP

LEGAL REPRESENTATIVE:
Wilding, Frances Ward et al (93562), Haseltine Lake Imperial House 15-19 Kingsway, London WC2B 6UD, (GB)

PATENT (CC, No, Kind, Date): EP 1063812 A2 001227 (Basic)
EP 1063812 A3 040714

APPLICATION (CC, No, Date): EP 2000304560 000530;

PRIORITY (CC, No, Date): JP 99174648 990621

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: H04L-009/08; H04L-009/32

ABSTRACT EP 1063812 A2

In a cryptographic method and equipment and a decrypting method and equipment according to the invention, the auxiliary code depending upon a

randomly determined numeric key and the result of encryption is included together with the result of encryption into a cryptogram. On decrypting, a cryptographic key is restored by using the numeric key restored according to the entire cryptogram and is utilized in the decryption. On the other hand, in another cryptographic method and equipment and another decrypting method and equipment according to the invention, on **encrypting** , **physical** characteristic information is scrambled and then encrypted. On this encryption, on the contrary, the result of decryption is descrambled. In these cryptographic method and equipment, together with decryption method and equipment, any small alteration made on the cryptogram causes a serious damage on the result of decryption. So, by applying these techniques to sending and receiving the physical characteristic information, their safety can be improved. On the other hand, in a remote identification system according to the invention, by **encrypting** the **physical** characteristic information by using a password as a cryptographic key, because of the fluctuation of the physical characteristic information, authenticating information represented as a different bit pattern at each identifying processing can be generated and sent to a transmission medium. So, by examining the equivalence between the result of decryption of the authenticating information and the registered reference information while considering the aforementioned fluctuation, the person can be reliably identified.

ABSTRACT WORD COUNT: 242

NOTE:

Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	001227	A2	Published application without search report
Search Report:	040714	A3	Separate publication of the search report
Change:	040825	A2	Legal representative(s) changed 20040709
Change:	040922	A2	Legal representative(s) changed 20040802
Change:	040825	A2	Legal representative(s) changed 20040709
Change:	040922	A2	Legal representative(s) changed 20040802
Examination:	041208	A2	Date of request for examination: 20041011

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200052	1128
SPEC A	(English)	200052	16063
Total word count - document A			17191
Total word count - document B			0
Total word count - documents A + B			17191

?